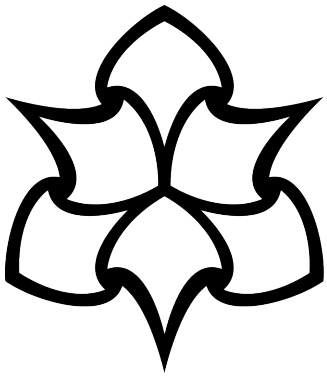

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 30, 2017, accepted September 24, 2017, date of publication October 2, 2017, date of current version November 7, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2758646

QoS-Aware Frequency-Based 4G+Relative Authentication Model for Next Generation LTE and Its Dependent Public Safety Networks

SHEEBA BACKIA MARY BASKARAN[1], GUNASEKARAN RAJA[1], (Senior Member, IEEE), ALI KASHIF BASHIR[2], (Senior Member, IEEE), AND MASAYUKI MURATA[3], (Member, IEEE)

[1]Department of Computer Technology, Anna University, Chennai 600025, India
[2]Faculty of Science and Technology, University of the Faroe Islands, FO-100 Faroe Islands, Denmark
[3]Graduate School of Information Science and Technology, Osaka University 565-0871, Japan

Corresponding author: Sheeba Backia Mary Baskaran (bobby_sheeba@yahoo.co.in)

The work of S. B. M. Baskaran and G. Raja was supported by the NGNLabs, Department of Computer Technology, Anna University, Chennai, India.

ABSTRACT Increasing demands for high-speed broadband wireless communications with voice over long term evolution (LTE), video on demand, multimedia, and mission-critical applications for public safety motivate 4th-generation (4G) and 5G communication development. The flat IP-based LTE and LTE-Advanced technologies are the expected key drivers for 5G. However, LTE, with its elapsed security mechanism and open nature, leaves a huge loophole for intruders to jeopardize the entire communication network. The time- and bandwidth-consuming authentication procedure in LTE leads to service disruptions and makes it unfit for public safety applications. To cater the prevailing LTE security and service requirements, we propose the 4G plus relative authentication model (4G+RAM), which is composed of two dependent protocols: 1) Privacy-protected evolved packet system authentication and key agreement protocol for the initial authentication (PEPS-AKA) and 2) 4G plus frequency-based re-authentication protocol for the re-authentication of known and frequent users (4G+FRP). The 4G+RAM supports seamless communication with a minimum signaling load on core elements and conceals users' permanent identifiers to ensure user privacy. We simulate the proposed protocols for formal security verification with the widely accepted automated validation of Internet security protocols and applications tool. A comparative analysis of bandwidth consumption is also performed and proved that the proposed 4G+RAM outperforms the existing solutions.

INDEX TERMS Authentication overhead, dynamic LTE key, EPS-AKA, IMSI-protection, LTE, public safety, re-authentication.

I. INTRODUCTION TO LTE AND PUBLIC SAFETY SERVICES

The currently used high-resolution mobile devices such as smartphones and laptops evolved from monochrome devices with low processing capabilities. These smartphones and laptops with high processing capabilities, coupled with a scalable cache of the bandwidth-hungry applications, demand higher data rates and produce better user experiences. The key feature of the 4th-Generation (4G) network is its ability to support peak downlink data rates of upto1GB/sec. The amount of mobile data is forecasted to grow more than 500-fold by 2020, and this has propelled the worldwide 4G deployment [1]. Long-Term Evolution (LTE - release 11) and LTE-Advanced (LTE-A - releases 12 and beyond) are the major 4G wireless communication technologies that are recommended by the 3rd-Generation Partnership Project (3GPP). The 3GPP 4G technologies aim to satisfy the growing user needs for voice over IP, video on demand, and evolving Internet applications and service requirements. LTE remains highly significant and will continue to evolve to achieve the goal of a 5G network as a commercial reality [2].

LTE and LTE-A are likely to evolve in the 5G era as LTE radio access technology becomes accessible to 5G devices [3]. Therefore, LTE and LTE-A cellular networks

can render services to future generation 5G devices. Indeed, cellular networks have established footprints worldwide and can address the challenges of ubiquitous networks. Additionally, the future 5G technology depends on the Information and Communication Technology (ICT) ecosystem, which is essential for business, commercial needs, and Public Safety (PS); in turn, its growth depends on the global success of LTE. LTE broadband communication is gaining importance in emergency and rescue operations, where voice calls will remain an essential service, even for PS systems. These voice calls in PS systems rely on voice over LTE [4]. PS communication security is of paramount importance in public safety LTE (PS-LTE) networks, which includes confidentiality, authentication and user privacy management [5]. Furthermore, with the increasing demands for information security and privacy in daily life and businesses, the success of the PS-LTE depends on its security and service level [6].

II. LTE SECURITY VULNERABILITIES

Whenever a user device tries to access a network such as LTE, the authentication process is triggered. The subscriber and access networks' mutual authentication function in the LTE evolved packet system follows the Evolved Packet System Authentication and Key Agreement (EPS-AKA) protocol, in which the authentication server validate the subscriber's credentials at the core network to provide the requested access and the network is authenticated by the user's device. According to the EPS-AKA protocol, the subscribers' device must perform a complete authentication process with the access network irrespective of their access frequency, which leads to intolerable signaling overhead and service failure.

The accessibility of the LTE network to 5G devices with low latency requirements will affect its Quality of Service (QoS); the impact will be especially detrimental for LTE-dependent PS services. Additionally, EPS-AKA suffers from several vulnerabilities, such as disclosure of user identity, man-in-the-middle attack, Authentication Vector (AV) synchronization failure, high computational overhead and authentication delays [7], [8]. LTE and LTE-A, as flat IP-based architectures, are vulnerable to injection attack, modification attack on user plane traffic and more privacy attacks than UMTS and GSM networks [9], [10]. In EPS-AKA process, the attach request message sent by the User Equipment (UE) to the Mobility Management Entity (MME) and the authentication request message sent by the MME to the UE are sent unencrypted. This is the main reason for the open nature and security vulnerabilities in LTE.

The unencrypted attach request message containing the International Mobile Subscriber Identity (IMSI) is a major threat to user privacy and safety. IMSI catchers act as fake base stations that can cache the subscriber IMSIs that are sent on air during the authentication process [9]. Stingray and Trigger fish are two major technologies that are used to track subscribers and their IMSIs legally [11]. These technologies can do more than tracking: during the ongoing VoIP services, the callers and speakers, the time of the call, and the location

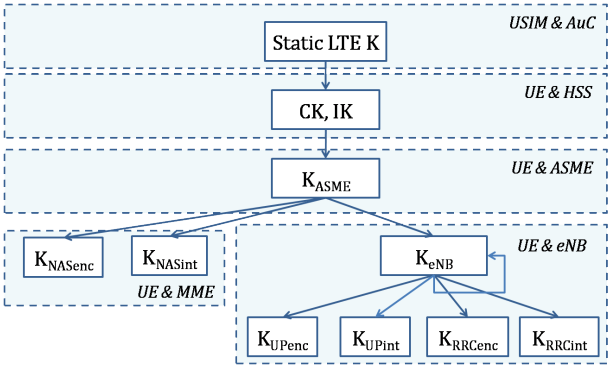

FIGURE 1. LTE key hierarchy.

from where the call initiated can also be identified. Stingray acts as a rogue base station that triggers the UE to initiate a communication through it. Once a successful communication is established, the rogue base station can capture the entire conversation with its technology. Triggerfish is a technology that can foresee the communication scenario for spying with its intelligence. These technologies in the hands of any intruder will be dangerous to mobile users' privacy and safety. These are the major critical issues that require urgent attention from researchers.

According to 3GPP TS 33.401, the entire key hierarchy is derived from the static key, LTE K, as shown in Figure 1. The Cipher Key (CK), Integrity Key (IK), Security master key (K_{ASME}), Non-Access Stratum (NAS) signaling encryption and integrity keys (K_{NASenc}, K_{NASint}), Radio Resource Control (RRC) signaling encryption and integrity keys (K_{RRCenc}, K_{RRCint}), and User plane encryption and integrity keys (K_{UPenc}, K_{UPint}) are the set of keys derived from the static LTE K. The Next hop (NH) key is the key derived by UE and MME to ensure forward security and $K_{eNB}*$ is the key derived by UE and eNB from the current K_{eNB} or fresh NH when performing a horizontal or vertical key derivation. The MME holds K_{ASME} (the MME base key), and it is not shared with the UE over direct transmission. This top-level key in the hierarchy is received by the access security management entity (ASME) from HSS and derived at the LTE user end based on the AV parameters it receives from the MME during the EPS-AKA authentication process. The MME is assumed to act as an ASME in every LTE access network. If any intruder compromises LTE K, then the entire LTE network can be tampered with [12]. As a result, security is potentially affected everywhere.

The proposed 4G+RAM with PEPS-AKA and 4G+FRP aims to achieve a better trade-off between security and QoS. To prevent the sniffing of users' permanent and temporary identifiers, which has critical security implications such as user tracking, user privacy, safety and reputation threats, the entire authentication and the re-authentication message exchange involving PEPS-AKA and 4G+FRP are protected in terms of confidentiality and integrity. Moreover, service failures and degradation due to the time-consuming

authentication procedure are significantly reduced by the 4G+FRP-based re-authentication. It ensures fast and seamless network access for LTE and PS-LTE users by avoiding HSS involvement and minimizes signaling between UE and network core elements. Overall, the 4G+RAM achieves secure and seamless communication for LTE and its dependent PS-LTE end users. No other significant research contribution has yet been made to PS-LTE security. Hence, this research work will be a thoughtful initiative that discusses the LTE enhancements to support 5G and PS services.

The organization of the paper is as follows. Section III presents a brief summary of the work related to LTE authentication and the security mechanism. Section IV presents the preliminaries that highlight the significant contribution of the proposed 4G+RAM for LTE and its dependent next-generation PS networks. Section V elaborates the proposed 4G+RAM with PEPS-AKA and 4G+FRP. Section VI presents a performance analysis based on the formal security verification of the proposed schemes with the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool and a comparative bandwidth consumption analysis against the existing schemes. It is inferred that the existing schemes that are considered in the comparative study are not bandwidth efficient; hence, the comparative analysis of the proposed systems is limited to authentication bandwidth consumption. Section VII discusses the security features of the proposed 4G+RAM framework, and finally, the conclusion is drawn in Section VIII.

III. RELATED WORK

This section gives a brief outline of the security issues and communication overhead issues in the LTE EPS-AKA as well as the corresponding solutions proposed to date and their shortcomings. Starting with the security issues related to IMSI, a static user identity guarantees confidentiality in an LTE access network. IMSI is necessary to clone any user. To establish a secure connection, it is mandatory to avoid the use of IMSI on air by replacing it with any other temporary identity, which is called the Temporary Mobile Subscriber Identity (TMSI) [13]. In contrast, the authentication protocols in recent research works transmit the unencrypted IMSI on air during the initial attach request, which allows intruders to tamper with the IMSI [9], [14]. Another major rising threat is redirection attack, where a fake Evolved Node B (eNB) redirects the user attach request to a foreign network when a user is eligible or intends to connect to its home network. In this case, the foreign network charges the mobile user based on a rate that is higher than the rate offered by the home network.

EPS Integrity algorithms (EIA), such as EIA1, EIA2, and EIA3, are being used in LTE. EIA2 is preferred for integrity protection in the proposed system as it utilizes AES as the underlying cipher and Cipher-based Message Authentication Code (CMAC) as the upper-level Message Authentication Code (MAC) structure, which has been proven to be secure. In contrast, EIA1 and EIA3 are polynomial MACs, which have the linear property and are prone to linear forgery attack and trace extension forgery attack [15], [16]. The lack of forward secrecy and vulnerability to man-in-the-middle attack are still security problems of LTE EPS-AKA, as an unencrypted authentication procedure is carried out between the UE and core network [9], [17], [18]. In the future, LTE systems are envisioned to support critical PS communication, where seamless communication between the victims and responders in tactile and emergency scenarios is required [5], [19].

Further, the issues related to authentication signaling and processing overhead due to the larger number of AV generations are analyzed. When a UE sends an access request to the LTE network in the EPS-AKA process, 'n' number of AVs are generated and stored at the HSS. If the UE does not stay within that access network any longer or if the UE does not visit the same LTE access network in the future, the stored AVs that correspond to the UE are discarded by the HSS. This approach of AV generation at the HSS without knowing the UE access frequency imposes unnecessary overload at the HSS [9]. The UE bandwidth consumption and authentication signaling overhead between the serving network and home network lead to authentication delay, which is one of the main problems in the existing system. The service access request is authenticated using the stored set of AVs and K_{ASME} without AKA execution. The in-sequence AV usage depends on the sequence number management schemes. Usually, this approach leads to re-synchronization problems due to the interleaving use of AVs. Therefore, when an AV is used for authentication shortly after its retrieval from the HSS, the re-synchronization problem in the EPS system can be avoided [20]. Moreover, caching the AV set imposes huge storage overhead in the UE and HSS. Additionally, if the authentication process for access provision depends completely on a remote backend server such as the HSS/Authentication Center (AuC), the access provision will be delayed and, moreover, the network partition will always result in denial-of-service attacks on the legitimate users. In the Ensure Confidentiality Authentication and Key Agreement protocol, many cryptographic operations are involved, which increases the computational overhead and complexity of the authentication process. Moreover, 'n' AVs are created by the HSS for use in future handovers, which is a burden to the HSS [21].

A few group-based and other solutions to minimize the authentication overhead and signaling congestion in the access network are discussed as follows. A group-based security protocol for Machine Type Communication is proposed, where the devices in a site are grouped to form a binary tree, with a group leader, where a set of leaders are included among other members to represent the group to the core network for performing authentication. During multiple initiations to avoid a collision, each leader waits for a random amount of time before initiating the first message. This random waiting process among the group leaders eventually increases the network access time of the mobile user, which is intolerable [22].

A Group-based Anonymity Handover Authentication Protocol scheme and a dynamic policy updating scheme for LTE-A involve huge computational cost [23], [24]. An enhanced EPS-AKA (EEPS-AKA) scheme introduces a one-way key function, predefined encryption function and a unique key identifier to enhance LTE security. It claims that for users possessing security context, authentication at the serving network is enabled instead routing the authentication process to the home network, thereby minimizing the communication overhead. However, the major drawback of this scheme is that the security context sharing process for the mobile user has not been discussed [25].

The summarized research contributions are unable to address the critical security and QoS requirements of the LTE system. Therefore, the current time-consuming authentication in LTE and security flaws require an effective viable solution, such as the proposed 4G+RAM, to meet the growing demands of the broadband communication ecosystem. When LTE-A is considered, the proposed 4G+RAM authentication model for LTE can be extended with minimum modifications to work with LTE-A. Furthermore, as no vast changes to the core LTE functionality are anticipated; the basic core security mechanisms will continue to prevail in LTE-A. The only change in LTE-A is to introduce relay nodes, and this work is already underway. To support the proposed 4G+RAM authentication framework, a set of function identifiers are cached at the UE and MME ends. Caching the function identifiers does not impose any overhead on the MME, as it has the capability to store the non-access stratum security context during EPS Connection Management connected to EPS Connection Management idle transitions. In LTE, the current key size is 128 bits, and there is a wide possibility to extend the key size to 256 bits in the future; therefore, LTE has the space to evolve into a better ICT.

IV. PRELIMINARIES OF LTE-DEPENDENT PUBLIC SAFETY NETWORK

Two separate technologies, such as cellular networks (LTE) and PS networks, provide wide-area wireless communications. The exceptional success of LTE and its business impact has led to rapid innovations. The critical PS network that provides services for fire, police and ambulance was once a standalone and dedicated network, which is expected to function better, with enhancements to LTE [5]. Therefore, the 3GPP is working to foster a common technology that can render better service to both communities.

The PS standards, such as TETRA and P25, put forth a set of features that were not supported by cellular systems [26]. Currently, 3GPP works on LTE-based proximity services (TS 23.303) and the group call system for PS (TS 23.468). The LTE-based network, with fast access and seamless communication for PS, is considered the prime factor in this research work. The underlying LTE architecture remains the same, but the functionalities of the access and core network entities need to be enhanced to support the PS services. The proposed 4G+RAM-based access scenario is depicted in Figure 2. The 4G+RAM aims to complement seamless communication for critical PS services over LTE. It clearly shows that, similar to the existing EPS-AKA, the proposed initial PEPS-AKA-based authentication involves message exchanges with UE, MME (through eNB) and HSS, whereas the proposed 4G+FRP-based re-authentication limits HSS involvement; this, in turn, greatly reduces the network access time and HSS overload.

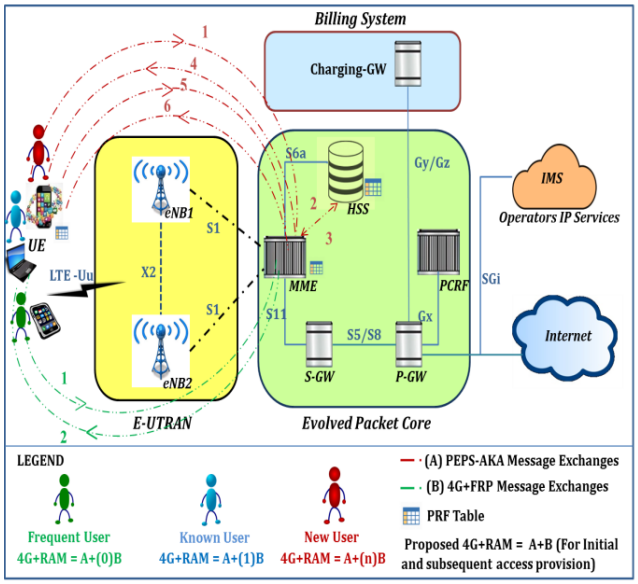

FIGURE 2. 4G+RAM-based access scenario in LTE architecture.

The authentication message exchanges of PEPS-AKA are depicted as red lines in Figure 2, and the authentication process flow from step 1 to step 6, is elaborated in Section V-A. The re-authentication message exchanges of 4G+FRP are depicted as green lines in Figure 2, and the re-authentication process flow, which involves steps 1 and 2, is elaborated in Section V-B.

The functions of the entities in the Evolved Universal Terrestrial Access Network (E-UTRAN) and Evolved Packet Core (EPC), shown in Figure 2, are briefly discussed as follows.

User Equipment: The UE holds a Universal Integrated Circuit Card with IMSI and Secret static LTE K. An LTE-Uu interface connects UE with eNB.

eNodeB: The E-UTRAN handles the radio access communication between the UE and EPC with the eNodeB (also known as eNB). An eNB is a base station that controls the mobile UE in the nearby cells. An eNB communicating with an active UE is known as a serving eNB. An eNB connects to other eNBs using an X2 interface and to the EPS using an S1 interface.

Home Subscriber Server: The HSS consists of the home Location Register and the AuC subsystem. The HSS holds a central database that manages all mobile subscriber information for user registration, handover, authentication, authorization, location updating, session routing, accounting, call control and AV forwarding to the MME. The HSS and MME

exchange subscription and authentication information using an S6a interface.

The Serving Gateway: The S-GW acts as a router and forwards the data from an eNB to the PDN gateway. The S-GW connects to the P-GW using an S5 interface during intra-LTE handover and using an S8 interface during LTE interworking handover.

The Packet Data Network Gateway: The P-GW communicates with the external world using an SGi interface. Here, the packet data network may be an Internet or an intra-operator packet data network for IP Multimedia Subsystem service provision.

The Policy Control and Charging Rule Function: The PCRF controls the flow-based charging functionalities in the policy control enforcement function of the P-GW using a Gx interface.

The Charging Gateway: The Charging-GW performs event-based and session-based charging for LTE applications and services. The charging GW communicates with the P-GW using Gy/Gz.

PRF Table: A PRF table with a set of PRFs needs to be maintained at every UE, eNB and HSS to support the flawless and efficient execution of the proposed 4G+RAM.

The merits of the proposed 4G+RAM are listed as follows.

1. Communication overhead due to transmission of the huge AV set from the HSS to the UE can be significantly reduced. Therefore, the AV synchronization problem and cache overhead at UE, MME and HSS are minimized.
2. The HSS is not involved in the re-authentication process when 4G+FRP is used as an extension to the proposed PEPS-AKA in 4G+RAM; hence, access delays in the LTE and PS-LTE networks are minimized.
3. All attach requests and response messages that are transmitted during the initial authentication and re-authentication processes are ciphered and integrity protected. Hence, 4G+RAM ensures protection against user identity theft, tracking, man-in-the-middle, synchronization, replay, denial-of-service (DoS), distributed denial-of-service (DDoS) and redirection attacks.
4. The dynamic LTE K generation ensures robust security in AV and K_{ASME} generation.
5. 4G+RAM provides a seamless and secure connection for the LTE network and its dependent critical PS network users.

V. PROPOSED 4G+ RELATIVE AUTHENTICATION MODEL: (4G+RAM)

In this section, the proposed 4G+RAM authentication model, which resolves the problem of authentication latency and the corresponding service failure, is discussed in detail. Re-authentication is used to minimize authentication access latency and ensures seamless communication. The 4G+RAM process flow is shown in Figure 3. The 4G+RAM is composed of two dependent authentication protocols: PEPS-AKA and a low-latency 4G+FRP, which are used for authentication and re-authentication, respectively. The LTE users are classified into three categories: new users, known users, and frequent users. Every new user is authenticated with the proposed PEPS-AKA protocol, and each known user is authenticated initially with the PEPS-AKA protocol and then re-authenticated with a 4G+FRP-based fast access provision for one future network entry. Finally, the frequent users, who benefit the most, are initially authenticated with PEPS-AKA and then re-authenticated with a 4G+FRP-based re-authentication mechanism for '*n*' future accesses.

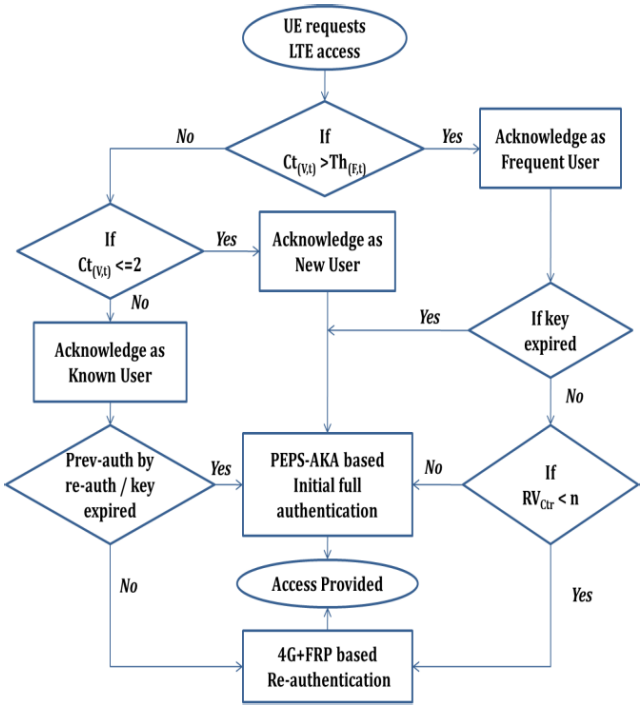

FIGURE 3. 4G+RAM process flow.

Based on our previous research contributions, the number of supported re-authentications '*n*' can range from 4 – 8 [27]. Here, each visit of a user to a particular LTE access network is counted, and the user is given fast network access during subsequent visits to the previously visited access networks. To determine whether an LTE user is a frequent visitor of a network, an access frequency threshold $Th_{(F,t)}$ and a network visit counter $Ct_{(V,t)}$ are maintained over time [0,t] for every LTE user.

With the user's first visit to a network, $Ct_{(V,t)}$ is initialized to '1', and with every successive visit to the same network, the value of $Ct_{(V,t)}$ is incremented. At time '*t*', for any LTE user, if $Ct_{(V,t)}$ equals $Th_{(F,t)}$, then that particular user is recognized as a frequent visitor. $Th_{(F,t)}$ is some upper bound value, and if this value is kept low, it can serve a wider subset of the LTE and PS-LTE population. The Re-authentication Vector Counter (RV_{Ctr}) for every frequent visitor denotes the number of successful re-authentications among '*n*' available re-authentications; RV_{Ctr} can take values up to '*n*'.

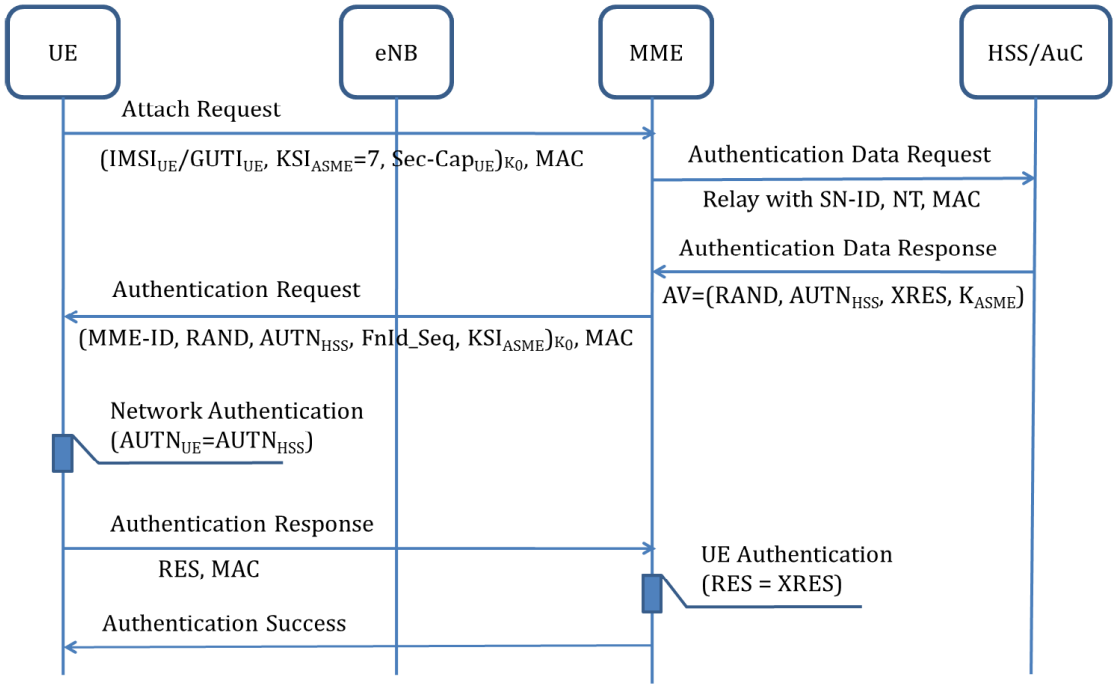

FIGURE 4. PEPS-AKA message exchange.

The PEPS-AKA and 4G+FRP authentication procedures are detailed in the following sections.

A. INITIAL AUTHENTICATION WITH PEPS-AKA

The message flow of the PEPS-AKA protocol is shown in Figure 4, and the steps involved in the PEPS-AKA-based authentication procedure are summarized as follows.

1. Initially, for a new user, when a UE attempts to connect with an LTE network, a confidentiality- and integrity-protected Attach Request is sent from the UE to the MME through an eNB with the IMSI, security capability and Key Selection Identifier (KSI_{ASME}) = 7. The Initial Attach Request message in addition contains an unconcealed and integrity protected dummy IMSI related to the users' IMSI to support user identification at the network side. The dummy IMSI is pre-shared using the USIM/UICC along with the secret K at UE and HSS. For known and frequent users, the Globally Unique Temporary Identifier (GUTI) is used instead of the IMSI. KSI_{ASME} is a 3-bit value ranging from 0 ("000") to 7 ("111"), where $KSI_{ASME} = 7$ indicates that the UE has no authentication key, which triggers the PEPS-AKA procedure.
2. The MME receives the Attach Request and sends an Authentication Data Request message, along with the Serving Network Identifier (SN-ID) and Network Type (NT), to the HSS and requests an Authentication Vector (AV) for the UE.
3. Upon receiving the Authentication Data Request, the HSS verifies the SN-ID, and if it is found to be genuine, the HSS retrieves the UE's secret key (LTE K) from its database and generates a single AV. The AV is generated as shown in Figure 5 and sent to the MME along with the security key (K_0) in the Authentication Data Response message. During the PEPS-AKA process, K_0 and AV are generated from the static LTE K, and once a user has been acknowledged as a frequent user, K_0 and AV are generated from the dynamic LTE K. The 128 least significant bits of K_0 are reserved for

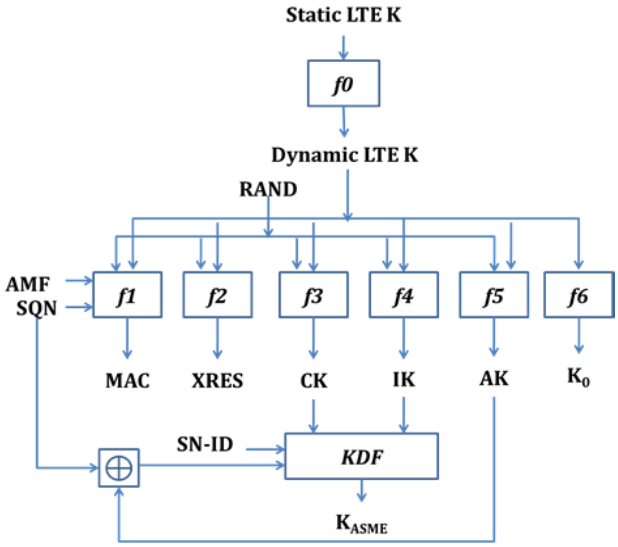

FIGURE 5. Cryptographic key material generation.

confidentiality protection, and the 128 most significant bits are reserved for integrity protection. The AV is composed of four parameters: a random number (RAND), expected response (XRES), K_{ASME} and authentication token (AUTN). Where '$f1 - f5$' shown in Figure 5, are the one-way hashing functions used to support AV generation. The sequence number (SQN) is generated by the HSS, and it is incremented by one for every round. Anonymity Key (AK) that is used to encrypt the SQN to ensure UE privacy protection when any eavesdropper tries to associate different executions of the authentication protocol with consecutive SQNs with the same mobile user. The Authentication Management Field (AMF) is configured in USIM and the operator's database in AuC. Thus, AUTN is computed as ((SQN XOR AK)||AMF||MAC).

4. The MME sends the confidentiality- and integrity-protected Authentication Request with its MME-ID, RAND, AUTN of HSS, Function Identifier Sequence (FnId_Seq) and KSI_{ASME} to the UE. FnId_Seq is an optional parameter and is sent only for known and frequent users. KSI_{ASME} is used by the UE to generate a K_{ASME} value that is identical to that of the HSS. For every initial UE-HSS association, the secret LTE K is used, which is a predefined static key that is stored in the UE and HSS as a factory setting. For every successive association, a new Pseudo Random Function (PRF) is used to generate a dynamic LTE K to leverage the LTE security. Therefore, the initial PRF identifier in the FnId_Seq parameter always denotes the PRF '$f0$' to generate the dynamic LTE K, and the rest of FnId_Seq contains the set of PRF identifiers to support 4G+FRP re-authentication key generation. For 4G+RAM execution between a single UE-MME pair, the dynamic LTE K varies and increases the overall security level. The MME stores FnId_Seq locally to support re-authentication. The dynamic LTE K generation using '$f0$' is further explained in Section V-B.
5. On the user side, the network authentication is performed with AUTN validation. If the network is found to be genuine, the Authentication Response (RES) is sent to the MME.
6. The MME validates the RES of the UE with the XRES in the AV received from the HSS. If the RES and XRES match, the UE is considered to be genuine. Thus, the MME authenticates the UE and an Authentication Success message is sent from the MME to the UE.

After a successful mutual authentication, the K_{ASME} generated by the HSS will also be generated by the UE, which is a top-level key (also known as an anchor key) that is used to secure LTE communication. Post PEPS-AKA authentication, the non-access stratum security mode command procedure and access stratum command procedures follow procedures that are similar to those of the existing LTE system.

The idea behind the proposed 4G+FRP is to use the K_{ASME} generated during the initial PEPS-AKA authentication as a seed for the predefined PRF according to the shared FnId_Seq to support Re-authentication K_{ASME} (r-K_{ASME}) generation at the UE and MME for a successful re-authentication.

The AES-based secure message authentication algorithm EEA2 is used for confidentiality protection, and EIA2 is used for integrity protection. EIA2 uses AES as the underlying cipher and CMAC as the MAC structure, which is extensively analyzed and proven to be secure. The PRF 'f6' is pre-shared and stored with the LTE K as the factory settings.

B. RE-AUTHENTICATION WITH 4G+FRP

The re-authentication process involves a single round-trip-time authentication, which is described as follows.

4G+FRP:
UE→MME (Attach Request):
$(GUTI_{UE}, \text{R-Id}, RV_{Ctr}, \text{r-}K_{ASME})_{K_R}$, $(GUTI_{UE}, \text{R-Id}, \text{Fn-Id}, RV_{Ctr}, \text{r-}K_{ASME})_{EIA2}$, T

MME→UE (Attach Response):
Re-authentication Success/Failure

1. The UE sends an Attach Request, with a re-authentication vector to the MME (through an eNB) during re-authentication. The re-authentication vector consists of a cipher- and integrity-protected GUTI, Re-authentication Identifier (R-Id), RV_{Ctr}, Re-authentication Key (r-K_{ASME}) and Timestamp (T). 'T' ensures the freshness of the message. R-Id is generated by both UE and MME, and it is unique to each UE and eNB pair. R-Id is generated by truncating the K_{ASME} value that is generated during the initial PEPS-AKA authentication. RV_{Ctr} denotes the number of re-authentications being carried out for a known or frequent visitor. To generate r-K_{ASME}, the UE initially fetches an Fn-Id that corresponds to RV_{Ctr} from the pre-shared FnId_Seq. The Fn-Id uniquely identifies a PRF in the order of the received FnId_Seq. A PRF table has a set of PRFs along with the received FnId_Seq and corresponding user R-Id that is maintained for every UE and eNB pair. The security key K_R and r-K_{ASME} generation shown in Figure 6(a)and 6(b) are pre-processes at the UE to send the attach request to the MME. The 128 least significant bits of K_R are reserved for confidentiality protection, and the 128 most significant bits are reserved for integrity protection of the 4G+FRP message exchanges.
2. Upon receipt of an Attach Request, the MME computes the corresponding K_R and r-K_{ASME} based on the received R-Id, RV_{Ctr} from the pre-shared FnId_Seq. If the r-K_{ASME} computed by the MME matches the received r-K_{ASME}, then a Re-authentication Success message is sent in the Attach Response to the UE.

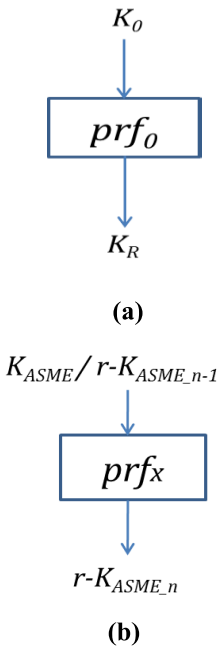

FIGURE 6. (a) Re-authentication message confidentiality and integrity protection key generation. (b) Re-authentication key generation.

For every re-authentication following an initial PEPS-AKA authentication K_{ASME} is used as a seed to generate the r-K_{ASME} key. In contrast, for every re-authentication following a re-authentication; i.e., n^{th} re-authentication following an $(n-1)^{th}$ re-authentication, r-$K_{ASME\text{-}n-1}$ is used as the seed to generate the r-K_{ASME-n} key. A set of PRFs is used as the key generation function. The PRF sequence used to generate subsequent r_K_{ASME} is pre-shared during the PEPS-AKA initial authentication phase.

Here, prf_x is a PRF, taken from a PRF set or sequence ("prf_0", prf_1, $prf_2 \ldots prf_x$, $prf_{x+1} \ldots prf_n$), where prf_0 is defined for two special purposes as (i) prf_0 is assigned as '$f0$' as shown in Figure 5 and that is used for dynamic LTE K generation, with the static LTE K as the seed after a normal authentication phase and the previously generated dynamic LTE K as the seed for the key hierarchy after a known authentication phase; and (ii) prf_0 is used for encryption key (K_R) derivation during re-authentication with K_0 as the seed. The remaining PRFs, from prf_1 to prf_n, are used in the order specified in FnId_Seq to derive the subsequent re-authentication keys (r-K_{ASME}).

A PRF that has been used once is not reused for r-K_{ASME} generation during a 4G+RAM cycle. Hence, the r-K_{ASME} is unique for a UE-eNB pair in its 4G+RAM duration. Additionally, as Fn-Id is not transmitted during the authentication request, r-K_{ASME} is highly secure. The various 4G+FRP parameters, along with their bit sizes, are presented in Table 1.

TABLE 1. Parameters and bit sizes of the re-authentication vector.

Parameter	Size (in bits)
$GUTI_{UE}$	80
R-Id	32
RV_{Ctr}	3
r-K_{ASME}	256
Fn-Id	3
T	16

VI. PERFORMANCE ANALYSIS

A. FORMAL SECURITY VERIFICATION

AVISPA is used with Security Protocol ANimator (SPAN) to validate the security properties of various 3G and 4G security protocols that were discussed in recent research works [28], [29]. As AVISPA provides a high level of assurance to both developers and users of next-generation security protocols, the proposed PEPS-AKA and 4G+FRP are validated using the AVISPA tool. The proposed protocols are modeled with the High-Level Protocol Specification Language (HLPSL). The HLPSL models the communicating entities UE, MME and HSS in different roles and specifies their behaviors with defined state machines [30]. Every protocol's HLPSL is composed of sections such as the role, session, goal and environment. The goal encompasses the authentication and secrecy goal of the protocols. The Dolev-Yao intruder model is set up to validate the resistance of PEPS-AKA and 4G+FRP to various intruder attacks. Before this, the Dolev-Yao model is given knowledge about various sessions in the protocol. With the gained intruder knowledge, the Dolev-Yao model attempts to analyze, intercept, inject and modify the exact message exchanges by impersonating a legitimate user [31].

All message exchanges in the proposed PEPS-AKA and 4G+FRP are encrypted with security keys K_0 and K_R using the EEA2 encryption algorithm and integrity protected with the EIA2 integrity algorithm, respectively. The goal sections of PEPS-AKA and 4G+FRP verify the secrecy of keys K_0 and K_R during the authentication and re-authentication intruder simulations, respectively, under the Dolev-Yao attack model. It also verifies the authentication goal between UE and HSS in PEPS-AKA and authentication goal between UE and MME in 4G+FRP. The intruder simulations of PEPS-AKA and 4G+FRP are shown in Figures 7 and 8, respectively.

The corresponding outputs from the back-end servers On-the-Fly Model Checker (OFMC), SAT-based Model Checker (SATMC) and Constrained Logic-based Attack Searcher (CL-AtSe) indicate that our proposed PEPS-AKA and 4G+FRP are safe under intruders' security attacks and satisfy the specified security goals. The sample output from the OFMC back-end server is shown in Figure 9. The related state-space tree construction by the OFMC [32] and the depth of attack analysis are shown in term of visited nodes and plies respectively.

B. BANDWIDTH CONSUMPTION ANALYSIS

This section defines the fluid-flow mobility model for the LTE system to determine the UE network boundary crossing rate and dwell time within a given LTE access network where

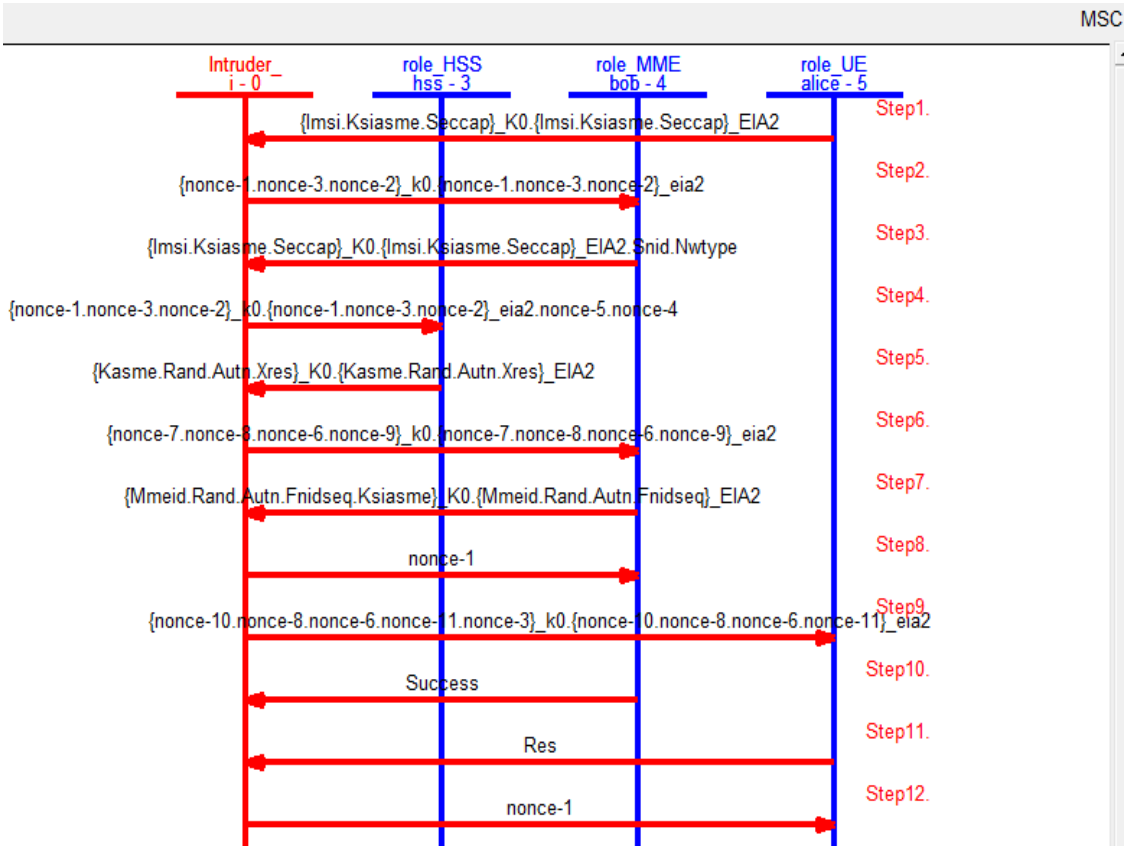

FIGURE 7. PEPS-AKA intruder simulation.

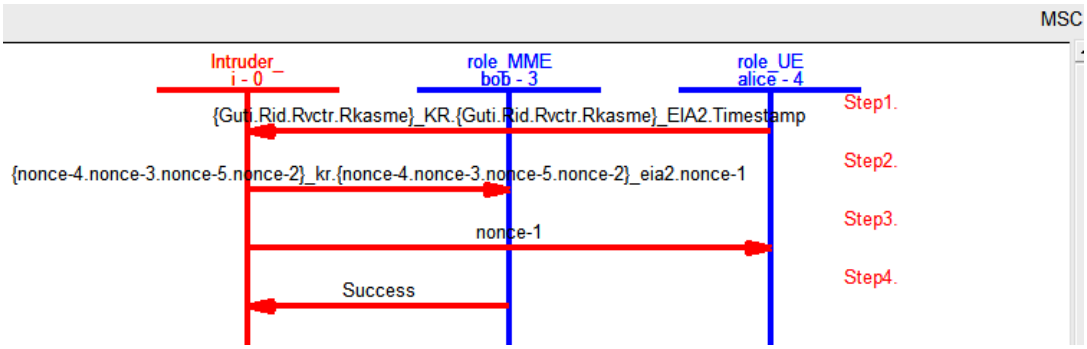

FIGURE 8. 4G+FRP intruder simulation.

the PEPS-AKA mechanism is triggered. The authentication overhead of PEPS-AKA and its bandwidth consumption are analyzed using the defined fluid-flow mobility model. The model describes the amount of data flow out from the LTE access region, which is directly proportional to the density of the mobile user population within the LTE access region, the average speed of a mobile user with respect to the direction (v), and the length (L) of the registration area boundary. It is assumed that the directions of movement of the mobile users are uniformly distributed over $[0,2\pi]$, and the mobile users are uniformly populated with a density of ρ. Therefore, the rate of registration area crossing by any mobile user is given by

$$R_{LTE} = \frac{\rho v L}{\pi} \tag{1}$$

When the fluid-flow mobility model is considered to analyze the PEPS-AKA authentication bandwidth consumption, various assumptions, which are presented in Table 2, are suggested by various research works, such as [25] and [33].

Based on the assumptions shown in Table 2 and equation (1), the rate of mobile UEs (arrival rate of UEs for

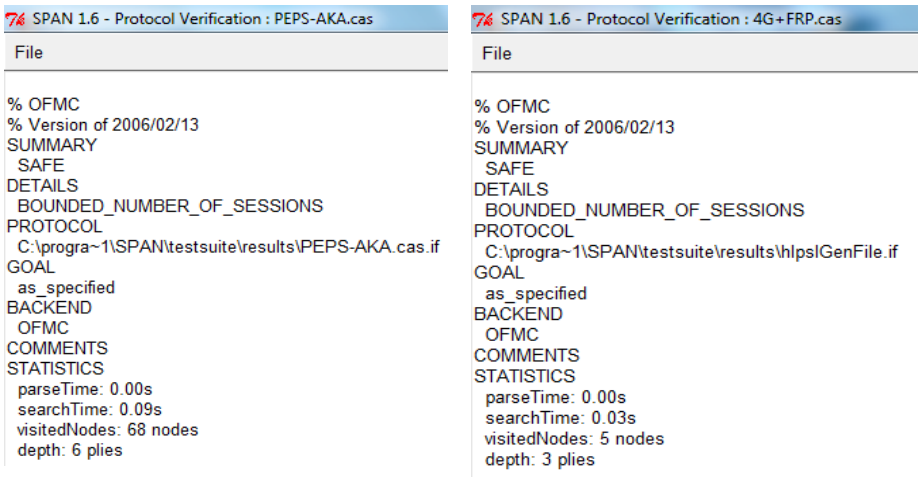

FIGURE 9. PEPS-AKA and 4G+FRP security results reported by OFMC.

TABLE 2. Parameters involved in bandwidth consumption analysis.

Parameter	Value
Mean density of mobile UEs (ρ)	390 units / sq.km
Total number of mobile UEs	(128)*(57.4)*(390) = 2.87 million
Square registration area	57.4 sqr.km
Average call initiation / Average call termination	1.4/hr/UE
Average speed of mobile users	5.6 km/hr
Total registration areas per LTE serving network	128
Border length	30.3 km

registration per access region) crossing an access region can be computed as equation (2).

$$R\_LTE = \frac{(30.3km \times 5.6km/s \times 390units/sq.km)}{3600\pi} = 5.85\ UEs/s. \quad (2)$$

The computed registration rate is equal to the de-registration rate. Therefore, the number of users requesting access to the network per second is equivalent to the number of authentication requests for registration per second, and it is calculated as

$$R_{Auth} = R\_LTE\ {}^{*}Number\ of\ registration\ area\ in\ a\ serving\ network = 5.85\ \text{users/sec}^{*}128 = 748.8\ \text{users/s}, \quad (3)$$

where R_{Auth} is the arrival rate of mobile users at an LTE access network for registration following an authentication. Therefore, the MME should be able to manage the processes of authentication and location area updating for 749 mobile users/s. As with all conventional authentication mechanisms, the MME, along with the HSS, takes over the entire authentication and key management process. Therefore, there is a huge threat to the MME and HSS/AuC due to computational overhead.

The bandwidth consumption of PEPS-AKA can be computed from the authentication request arrival rate (R_{Auth}). Based on the rate of authentication request arrival and the authentication parameters given in Table 3, the total authentication bandwidth consumption ($Total\_BW_{Auth}$) can be calculated as shown in (4).

$$Total\_BW_{Auth} = Authentication\ Message\ Size\ {}^{*}No.\ of\ Authentication\ Request/s \quad (4)$$

To evaluate the optimal performance of the proposed PEPS-AKA protocol, computing the bandwidth utilization between the serving MME and HSS is sufficient. The HSS overhead and authentication delay are mainly due to excess message exchange between the MME and HSS. The size of a message exchanged between the MME and HSS in the conventional authentication mechanism is the sum of the sizes of the messages sent during AV request and AV reception. The bit sizes of the authentication parameters for message computation of SE-AKA and Enhanced AKA are taken from their corresponding research works [25], [34]. In previous works, it was proven that SE-AKA outperforms various other LTE authentication schemes, such as EPS-AKA, DEX-AKA, EAP-AKA, AP-AKA, X-AKA, Cocktail AKA, S-AKA and G-AKA [34], [35]. Therefore, the comparison of PEPS-AKA is limited to recently proposed and accepted research works, such as Enhanced AKA and SE-AKA. In conventional authentication schemes [25], [34], the size of a message transmitted between the MME and HSS is calculated as follows.

$$\begin{aligned} &Message\ size\ of\ SE\text{-}AKA \\ &= SNID + IMSI + [AV(RAND + XRES + AUTN + K_{ASME})^{*}n] \\ &= 48 + 64 + [(128 + 32 + 128 + 256)^{*}5] \\ &= 48 + 64 + 2720 = 2832\ \text{bits} \end{aligned} \quad (5)$$

TABLE 3. PEPS-AKA parameters and bit sizes.

Parameter	Size (in bits)	Parameter	Size (in bits)
IMSI	64	AUTN	128
KSI_{ASME}	3	RES	32
Sec-Capability	16	XRES	32
SN-ID	28	K_{ASME}	256
NT	4	MME-ID	128
RAND	128	FnId_Seq	30
MAC	128		

$$\begin{aligned} &Total\_BW_{Auth}\_SE\text{-}AKA \\ &= 2832\ bits \times 748.8/s \\ &= 2.022\ Mbits/s \end{aligned} \tag{6}$$

$$\begin{aligned} &Message\ size\ of\ Enhanced\text{-}AKA \\ &= 2^{*}SNID + 2^{*}KI + IMSI + M\text{-}ID + RAND_{UE} + S \\ &= 2^{*}48 + 2^{*}128 + 128 + 60 + 128 + 128 \\ &= 796\ \text{bits} \end{aligned} \tag{7}$$

$$\begin{aligned} &Total\_BW_{Auth}\_Enhanced\ AKA \\ &= 796\ bits^{*}748.8/s \\ &= 0.568\ Mbits/s \end{aligned} \tag{8}$$

During the initial authentication, except for the difference in bit size of messages transmitted between the UE, MME and HSS, the number of rounds for requesting AV is similar in existing schemes and the proposed PEPS-AKA. Here, we consider the size of the authentication message exchanged between the MME and HSS to evaluate the bandwidth consumption and HSS load. Therefore, the message size of the proposed PEPS-AKA between the MME and HSS is equal to the total number of authentication requests and response message exchanges.

$$\begin{aligned} &Size\ of\ PEPS\text{-}AKA\ message \\ &\quad = IMSI + SN\text{-}ID + NT + MAC + AV \\ &\qquad \times (RAND + AUTN + XRES + K_{ASME}) \\ &\quad = 64 + 28 + 4 + 128 + 128 + 128 + 32 + 256 \\ &\quad = 768\ \text{bits} \end{aligned} \tag{9}$$

$$\begin{aligned} &Total\_BW_{Auth}\_PEPS\text{-}AKA \\ &\quad = 768\ bits^{*}748.8/s \\ &\quad = 575078.4\ bits/sec \\ &\quad = 0.548\ Mbits/s \end{aligned} \tag{10}$$

As discussed in Section IV, 4G+RAM is a combination of PEPS-AKA and 4G+FRP. Therefore, the 4G+RAM authentication signaling overheads at the HSS for different authentication arrival rates are comparatively analyzed with those of existing schemes, such as SE-AKA and Enhanced EPS-AKA in Figures 10 and 11.

The existing schemes fetch 'n' AVs from the HSS, whereas the proposed PEPS-AKA fetches only a single AV from the HSS. Meanwhile, the MME sends the required FnId_Seq to the UE to support 'n' future accesses and the generation of the corresponding re-authentication vectors; therefore, the HSS load is very minimal and is balanced in 4G+RAM authentication and re-authentication compared to the existing schemes.

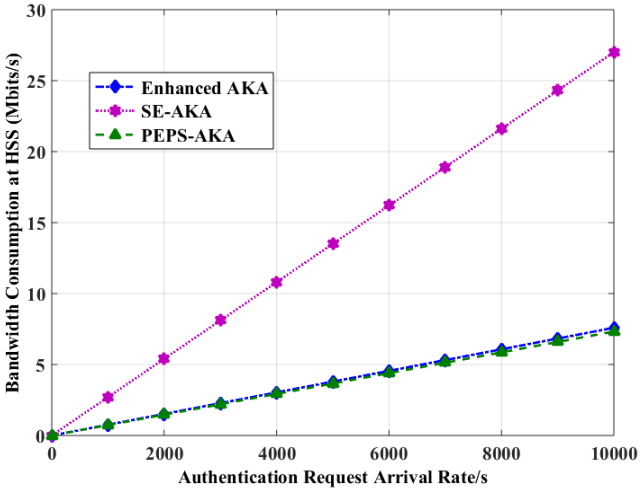

FIGURE 10. Comparison of HSS loads during initial authentication.

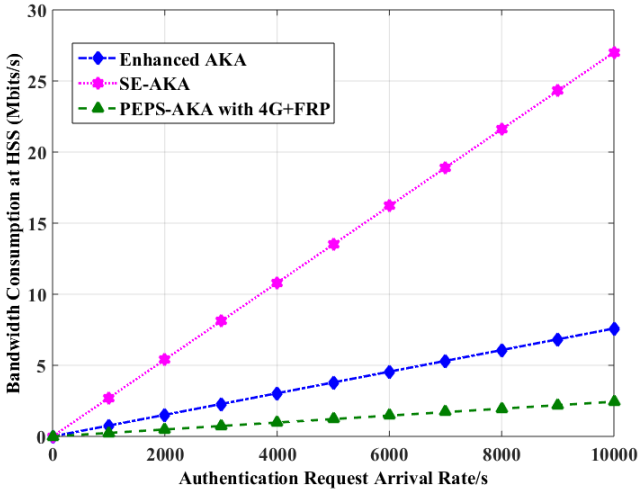

FIGURE 11. Comparison of HSS Loads during Session / Re-authentication.

Therefore, both the known- and frequent-user authentication processes of the proposed 4G+RAM greatly reduce the HSS and AuC overhead. This minimum re-authentication signaling renders fast access for LTE and critical PS-LTE users. No AVs for future access are generated during the initial authentication, but the required re-authentication vector is generated as and when required, without any delay at the MME itself; this eliminates the AV synchronization problem.

1) INITIAL AUTHENTICATION FOR A NEW USER

To demonstrate the optimal performance of PEPS-AKA, a comparative analysis based on the entire authentication bandwidth consumption is performed. The authentication overheads of PEPS-AKA, Enhanced AKA, and SE-AKA are computed in (11), (12), and (13) as follows.

m1: Attach request sent from UE to MME
m2: Authentication data / AV request from MME to HSS
m3: AV data response sent from HSS to MME
m4: Authentication request along with FnId_Seq sent from MME to UE.
m5: Authentication response sent from UE to MME

$$Bandwidth\ for\ PEPS\text{-}AKA = \prod_{i=1}^{5} M\,(i)\ ^{*}748.8/s \quad (11)$$

$$m1 = IMSI + KSI_{ASME} + SEC\text{-}Capability + MAC$$
$$m2 = IMSI + SN\text{-}ID + NT$$
$$m3 = AV(RAND, AUTN, XRES, K_{ASME})$$
$$m4 = MME\text{-}ID, RAND, AUTN_{HSS}, K_{ASME}, FnId\_Seq, MAC$$
$$m5 = RES$$

$$Bandwidth\ for\ Enhanced\ AKA = \prod_{i=1}^{5} M\,(i)\ ^{*}748.8/s \quad (12)$$

$$m1 = SNID + KI + IMSI + M\text{-}ID + RAND_{UE}$$
$$m2 = 2^{*}SNID + KI + IMSI + M\text{-}ID + RAND_{UE}$$
$$m3 = KI + S$$
$$m4 = KI + RAND_{MME} + AUTH$$
$$m5 = RES$$

Based on the assumptions of the fluid-flow model given in Table 2, a serving network consists of 128 registration areas. According to the SE-AKA scheme [34], each registration area is considered as a group, where one UE in each group is assumed to perform full authentication, representing all group members, whereas the other UEs may send or receive *m*1, *m*5, *m*4, etc. Each group (G) is assigned a group number '*j*'. The SE-AKA bandwidth is calculated as follows.

$$Bandwidth\ for\ SE\text{-}AKA = 128/sec^{*}\prod_{i=1}^{5} m\,(i) + (748.8-128)\ ^{*}(m1 + m4 + m5 - MACGj - TGj) \quad (13)$$

$$m1 = ID_{Gj} + TID_{ME} + R_{ME} + MAC_{Gj} + T_{Gj}$$
$$m2 = ID_{Gj} + TID_{ME} + R_{ME} + MAC_{Gj} + T_{Gj} + LAI$$
$$m3 = R_{HSS} + R_{ME} + AMF + 748.8/128(SV_{ME} + TID_{ME})$$
$$m4 = ID_{MME} + ID_{Gj} + TID_{ME} + MAC_{MME} + R_{HSS} + R_{MME} + R_{ME} + AMF + aP$$
$$m5 = MAC_{ME} + bP$$

2) AUTHENTICATION AND RE-AUTHENTICATION FOR KNOWN AND FREQUENT USERS

Once the UE is registered, in both Enhanced-AKA and SE-AKA, the AV is made available in the serving network; hence, the HSS is not involved in fetching the AV. However, this AV availability at the UE side and the MME side will result in a huge security loophole when the UE is compromised. In turn, according to the proposed authentication model, in both the proposed PEPS-AKA and 4G+FRP, the AVs and re-authentication vectors are generated as and when required on the go by fetching from the HSS and with the pre-shared FnId_Seq at the MME, respectively. Therefore, the HSS involvement is reduced to a great extent. The bandwidth consumptions of PEPS-AKA and 4G+FRP are computed based on the authentication request arrival rate [36]. As mentioned in previous research, the authentication request arrival rate in an intra-domain handover is expressed as

$$\lambda_1 = \sum_{r=1}^{4} \lambda_u P_r \left(\left[\overline{N_a}\right] - 1\right) \quad (14)$$

where λ_u, is the call arrival rate, P_r is the probability that a UE initiates a network access, and the connection lasts until a UE moves out of the current access domain. $\overline{N}_a$ is the average number of access areas passed by a UE. When the UE call arrival rate λ_u follows a Poisson distribution, then the average number of intra-domain handover authentications is $[\overline{N}_a]-1$. Let λ_2 be the rate of arrival of session authentications. It is the same as the UE call arrival rate [36]. Therefore, $\lambda_2 = \lambda_u$.

The bandwidth consumption for PEPS-AKA and enhanced AKA are computed as

$$BW\_PEPS\text{-}AKA = (\lambda 1 + \lambda 2)^{*}(m1 + m4 + m5) \quad (15)$$

The bandwidth consumption for 4G+FRP is computed as

$$BW\_4G + FRP = ((\lambda 1 + \lambda 2)^{*}(m1' + m2') \quad (16)$$

where,

m1': Authentication request from UE to MME

m2': Authentication request from MME to UE

The bandwidth consumption for SE-AKA is computed as

$$BW\_SE\text{-}AKA = (\lambda 1 + \lambda 2)^{*}(m1 + m4 + m5) - (\lambda 1 + \lambda 2)\ ^{*}(MAC_{Gj} + T_{Gj}) \quad (17)$$

Using the bandwidth consumptions of various protocols, calculated from (15)-(17), and the authentication arrival rate in an access network, as given in (14), a comparison among the authentication arrival rates and the corresponding bandwidth consumptions for PEPS-AKA, 4G+FRP, Enhanced-AKA, and SE-AKA is performed as depicted in Figures 12 and 13. As in [25] and [36], a few assumptions are made: $\lambda_u = 8.7$/sec/registration area, $P_r = 1$ and $\overline{N}_a = 10$.

VII. DISCUSSION ON SECURITY FEATURES

A. USER PRIVACY PROTECTION

The authentication requests and responses in PEPS-AKA and 4G+FRP are encrypted, and the IMSI is sent only during the initial authentication. During every re-authentication, instead of the IMSI, the GUTI is sent in the access request. Therefore, as the rate of on-the-air IMSI transmission decreases and every attach request message containing the IMSI is encrypted and integrity-protected, the possibility of IMSI tampering, user tracking, or user information acquisition becomes negligible.

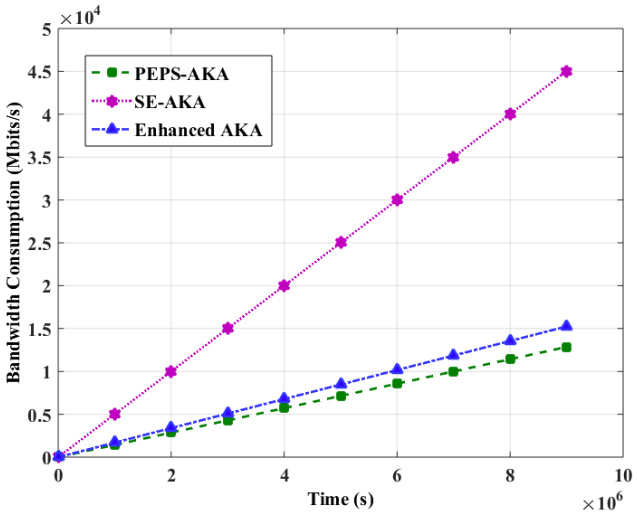

FIGURE 12. Comparison of bandwidth consumption for initial authentication.

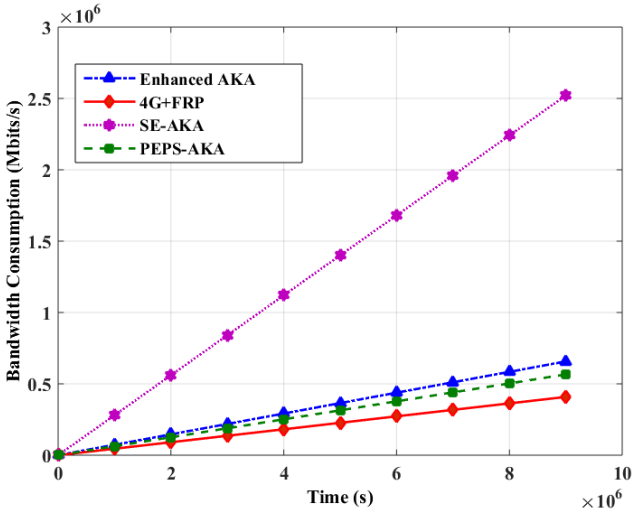

FIGURE 13. Comparison of bandwidth consumption for session / handover authentication.

B. SECURITY AGAINST MAN-IN-THE-MIDDLE ATTACK

To perform a successful man-in-the-middle attack, an intruder needs to tamper with the IMSI of a legitimate user. With the IMSI of any legitimate user, the intruder can send an attach request message to receive the valid AV from the HSS. However, in PEPS-AKA and 4G+FRP, the IMSI cannot be fetched at any level, as the IMSI transmitted during the authentication process is confidentiality and integrity protected. Moreover, during every re-authentication, the GUTI is sent as the UE identifier instead of the IMSI, so a man-in-the-middle attack is not feasible. Additionally, the IMSI cannot be cached or tampered with when using any IMSI catching device.

C. RESISTANCE TO RE-DIRECTION ATTACK

During the initial authentication, on receiving the attach request message, only the MME sends the SN-ID in an authentication data request to the HSS. As both the MME and HSS reside in the secured backhaul connection network, tampering is not possible at this stage. Moreover, the intruder can impersonate only a genuine eNB to perform a re-direction attack. As an eNB does not initiate any attach request in the PEPS-AKA process, a fake eNB cannot modify the SN-ID. Additionally, during the 4G+FRP process, re-authentication is initiated only with trusted and previously authenticated genuine eNBs, and no new eNB can initiate 4G+FRP. Therefore, a re-direction attack is not feasible.

D. SOLUTION TO THE SINGLE-KEY PROBLEM

The pre-shared static LTE K in the UE and HSS is the source key for deriving all subsequent key materials in the LTE network. If the static LTE K is compromised, then all other keys can be retrieved. Taking this into consideration, in 4G+RAM, the static LTE K is used only once during the very first initial authentication, and for every successive access dynamic, LTE K is used to generate the entire LTE key hierarchy. Thus, the single-key problem is addressed effectively.

E. SECURITY AGAINST RE-PLAY ATTACK

The entire communication between any UE and MME is protected with the anchor key, K_{ASME}. It is dynamically generated with a different set of PRFs, so no cached K_{ASME} can be re-used for future communication. Every attach request corresponding to the re-authentication contains a timestamp value, which ensures the freshness of the message and prevents replay attempts.

F. DE-SYNCHRONIZATION ATTACK

The single AV generation in PEPS-AKA prevents the interleaving usage of AV which in turn avoids the de-synchronization attack. Moreover, this type of attack in MME prevents the timeliness of handover key management. It is a potential security flaw when the intruder compromises any security key. The proposed 4G+RAM uses the K_{ASME} that was previously generated to derive r-K_{ASME} with a different PRF, and if any authentication failure occurs, the secret LTE K is used to re-initiate the authentication with PEPS-AKA. Additionally, during the re-authentication phase, if any network error occurs, the UE can re-initiate a 4G+FRP-based re-authentication with the unused set of Fn-IDs in the order specified by the received FnId_Seq. Therefore, no communication failure occurs at any level.

G. SIGNALING OVERHEAD OPTIMIZATION

During every initial authentication, a single AV is fetched, instead of 'n' AVs, from the HSS, and HSS involvement in the re-authentication process is completely eluded. These two enhancements reduce the signaling overhead and bandwidth consumption in the LTE access network significantly.

H. PERFECT FORWARD AND BACKWARD SECRECY

Dynamic LTE K-based key generation ensures perfect forward and backward secrecy without imposing any overhead

on the existing system. Moreover, the PRFs used to generate K_{ASME} are not logically related or dependent. Therefore, if any authentication key is obtained, the previous keys and successive keys cannot be derived at any level, so all past and future communications are made safe.

I. DENIAL-OF-SERVICE ATTACK

The hackers execute Denial-of-Service (DoS) attack by cloning the legitimate UEs' identification information (IMSI) to send multiple attach request messages to the LTE access network simultaneously along with the legitimate UEs' attach request message. Where the MME will be overwhelmed by this kind of DoS attack and the legitimate UE's attach request will be denied. The LTE EPS-AKA is prone to DoS attack due to lack of confidentiality protection and integrity protection. Whereas the proposed 4G+RAM is resistant towards DoS as both PEPS-AKA and 4G+FRP carrying subscriber identification information are confidentiality and integrity protected.

J. DISTRIBUTED DENIAL-OF-SERVICE ATTACK

Using a technique similar to botnets that attacks websites to achieve distributed denial-of-service (DDoS) attack, it is also possible for the hackers to overwhelm the LTE cellular networks to shut it down. To execute a successful DDoS attack, the hackers need to clone the subscriber identification information (IMSI/GUTI) from SIM cards/USIM from thousands of UEs and then make multiple roaming calls from different geographical locations with different handsets. DDoS in LTE will deliberately confuse the network with a mobile number that appears to be in thousands of places at once. But, the subscriber identification information in the proposed 4G+RAM will not be available to hackers as all the message exchange during PEPS-AKA and 4G+FRP are confidentiality and integrity protected.

VIII. CONCLUSION

The ever-growing mobile broadband network requires improved LTE support, which impacts every aspect of day-to-day life. LTE, as the key driver for 5G, needs significant research contributions to fix its security loopholes and reduce its signaling overhead. 4G+RAM is proposed as a solution to address the existing issues of the LTE system and make it a better information and communication technology ecosystem and to suit the growing demands of the next-generation 5G and critical PS systems. The entire authentication and re-authentication procedures involved in the proposed 4G+RAM are confidentiality- and integrity-protected with dynamic LTE K and thus overcome the critical security vulnerabilities of the LTE system, such as user tracking based on IMSI, redirection, and AV de-synchronization, and preventing man-in-the-middle and denial-of-service attacks. 4G+RAM minimizes the access latency, as the proposed PEPS-AKA and 4G+FRP involve minimal authentication signaling compared to other recent methods. This makes LTE the most suitable network for critical PS communications. However, proving latency improvement in terms of authentication time is outside the scope of this paper. Moreover, 4G+FRP offers fast and secure network access to known and frequents users and thus provides better QoS to a wide group of mobile users. The HSS is not involved in re-authentication; as a result, the HSS load is reduced. Additionally, the PEPS-AKA and 4G+FRP schemes are proven safe using the formal verification tool AVISPA. Thus, the proposed 4G+RAM with PEPS-AKA and 4G+FRP ensures privacy protection and seamless, secure communication in LTE and LTE-dependent future-generation PS networks.

REFERENCES

[1] W. H. Chin, Z. Fan, and R. Haines, "Emerging technologies and research challenges for 5G wireless networks," *IEEE Wireless Commun.*, vol. 21, no. 2, pp. 106–112, Apr. 2014.
[2] GSMA Intelligence. (Jan. 5, 2015). *Understanding 5G: Perspective on Future Technological Advancements in Mobile*. [Online]. Available: https://www.gsmaintelligence.com/research/?file=c88a32b3c59a11944a9c4e544fee7770&download
[3] E. H. Rachid and E. Javan. (Feb. 17, 2015). NGMN 5G White Paper, Next Generation Mobile Network Alliance. [Online]. Available: https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf
[4] T. Doumi *et al.*, "LTE for public safety networks," *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 106–112, Feb. 2013.
[5] L. Carlà, R. Fantacci, F. Gei, D. Marabissi, and L. Micciullo, "LTE enhancements for public safety and security communications to support group multimedia communications," *IEEE Netw.*, vol. 30, no. 1, pp. 80–85, Jan. 2016.
[6] Nokia Networks. *LTE Networks for Public Safety Services*. Accessed: Jul. 1, 2017. [Online]. Available: https://resources.ext.nokia.com/asset/200168
[7] K. A. Alezabi, F. Hashim, S. J. Hashim, and B. M. Ali, "An efficient authentication and key agreement protocol for 4G (LTE) networks," in *Proc. IEEE Reg. 10 Symp.*, Apr. 2014, pp. 502–507.
[8] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "LGTH: A lightweight group authentication protocol for machine-type communication in LTE networks," in *Proc. IEEE Global Commun. (GLOBECOM)*, Atlanta, GA, USA, Dec. 2013, pp. 832–837.
[9] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 283–302, 1st Quart., 2013.
[10] "5G Security—Scenarios and solutions," Ericsson, Stockholm, Sweden, White Paper Uen 284 23-3269, Jun. 2017, pp. 1–12, [Online]. Available: https://www.ericsson.com/assets/local/publications/white-papers/wp-5g-security.pdf
[11] L. Parks, "Rise of the IMSI catcher," *Media Fields J.*, no. 11, pp. 1–19, 2016.
[12] A. N. Bikos and S. Nicolas, "LTE/SAE security issues on 4G wireless networks," *IEEE Secur. Privacy*, vol. 11, no. 2, pp. 55–62, Mar./Apr. 2013.
[13] M. Abdeljebbar and R. El Kouch, "Fast authentication during handover in 4G LTE/SAE networks," *IERI Procedia*, vol. 10, no. 1, pp. 11–18, 2014.
[14] M. Bartock, J. Cichonski, and J. Franklin. (Apr. 2015). "LTE security—How good is it?" NIST, Gaithersburg, MD, USA, Tech. Rep. 3. [Online]. Available: https://www.rsaconference.com/writable/presentations/file_upload/tech-r03_lte-security-how-good-is-it.pdf
[15] T. Wu and G. Gong, "The weakness of integrity protection for LTE," in *Proc. 6th Conf. Secur. Privacy Wireless Mobile Netw.*, Apr. 2013, pp. 70–88.
[16] A. Zugenmaier and H. Aono, "Security technology for SAE/LTE," *NTT DOCOMO Tech. J.*, vol. 11, no. 3, pp. 27–30, 2009. [Online]. Available: https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol11_3/vol11_3_027en.pdf
[17] M. A. Andrabou, A. D. E. Elbayoumy, and E. A. El-Wanis, "LTE authentication protocol (EPS-AKA) weaknesses solution," in *Proc. IEEE Int. Conf. Intell. Comput. Inf. Syst.*, Dec. 2015, pp. 434–441.
[18] C.-K. Han and H.-K. Choi, "Security analysis of handover key management in 4G LTE/SAE networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 457–468, Feb. 2014.

[19] R. Favraud, A. Apostolaras, N. Nikaein, and T. Korakis, "Toward moving public safety networks," *IEEE Commun. Mag.*, vol. 54, no. 3, pp. 14–20, Mar. 2016.
[20] *Digital Cellular Telecommunications System (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security Architecture*, document ETSI TS 133 401 v12.15.0, Dec. 2015.
[21] J. B. Abdo, J. Demerjian, H. Chaouchi, and G. Pujolle, "EC-AKA2 a revolutionary AKA protocol," in *Proc. IEEE Int. Conf. Comput. Appl. Technol. (ICCAT)*, Sousse, Tunisia, Jan. 2013, pp. 1–6.
[22] D. Choi, S. Hong, and H.-K. Choi, "A group-based security protocol for machine type communications in LTE-advanced," in *Proc. IEEE INFOCOM*, Toronto, ON, Canada, Apr./May 2014, pp. 161–162.
[23] J. Cao, H. Li, and M. Ma, "GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., Sep. 2015, pp. 3020–3025.
[24] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A Networks," *IEEE Internet Things J.*, vol. 3, no. 3, pp. 408–417, Jun. 2016.
[25] F. B. Degefa, D. Lee, J. Kim, Y. Choi, and D. Won, "Performance and security enhanced authentication and key agreement protocol for SAE/LTE network," *Comput. Netw.*, vol. 94, no. 1, pp. 145–163, Jan. 2016.
[26] CISCO. (2012). *Broadband Revolution: Roadmap for Safety and Security Mobile Communication Services*. [Online]. Available: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/emergencyresponder.pdf
[27] R. Gunasekaran, S. B. M. Baskaran, D. Ghosal, and P. Jayashree, "Reduced overhead frequent user authentication in EAP-dependent broadband wireless networks," *Mobile Netw. Appl.*, vol. 21, no. 3, pp. 523–538, Jun. 2016.
[28] V. Odelu, A. K. Das, and A. Goswami, "SEAP: Secure and efficient authentication protocol for NFC applications using pseudonyms," *IEEE Trans. Consum. Electron.*, vol. 62, no. 1, pp. 30–38, Apr. 2016.
[29] L. Chengzhe, L. Hui, Z. Yueyu, and C. Jin, "Simple and low-cost Re-authentication protocol for HeNB," *IEEE China Commun.*, vol. 10, no. 1, pp. 105–115, Jan. 2013.
[30] A. Muñoz, A. Maña, and D. Serrano, "AVISPA in the validation of ambient intelligence scenarios," in *Proc. IEEE Int. Conf. Availab., Rel. Secur.*, Fukuoka, Japan, Mar. 2009, pp. 1–7.
[31] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Info. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 2008.
[32] D. Basin, S. Modersheim, and L. Vigano, "An on-the-fly model-checker for security protocol analysis," (Lecture Notes in Computer Science), vol. 2808. Springer, 2003, pp. 253–270.
[33] S. Mohan, "Privacy and authentication protocols for PCS," *IEEE Pers. Commun.*, vol. 3, no. 5, pp. 34–38, Oct. 1996.
[34] C. Lai, H. Li, R. Lu, and X. S. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," *Comput. Netw.*, vol. 57, no. 17, pp. 3492–3510, Dec. 2013.
[35] Z. Faigl, J. Pellikka, L. Bokor, and A. Gurtov, "Performance evaluation of current and emerging authentication schemes for future 3GPP network architectures," *Comput. Netw.*, vol. 60, no. 1, pp. 60–74, Feb. 2014.
[36] W. Liang and W. Wang, "A quantitative study of authentication and QoS in wireless IP networks," in *Proc. IEEE Comput. Commun. Soc. (INFOCOM)*, Miami, FL, USA, Mar. 2005, vol. 2. no. 1, pp. 1478–1489.

SHEEBA BACKIA MARY BASKARAN received the B.Tech. degree in information technology from Anna University, Chennai, and the M.E. degree in computer science and engineering from Anna University, Coimbatore. She is currently pursuing the Ph.D. degree with the NGNLabs, Department of Computer Technology, Anna University-MIT Campus, Chennai. She is also a Consultant with NEC India. She is carrying out her research in security solutions for broadband wireless networks. Her research interest includes WiMAX, LTE, LTE-A, 5G Security, and MAC layer protocol design. She was a recipient of the UGC-Maulana Azad National Fellowship.

GUNASEKARAN RAJA (M'08–SM'17) received the B.E. degree in computer science and engineering from the University of Madras in 2001, the M.E. degree in computer science and engineering from Bharathiyar University in 2003, and the Ph.D. degree with the Faculty of Information and Communication Engineering, Anna University, Chennai, in 2010. He was a Post-Doctoral Fellow with the University of California at Davis, Davis, USA, from 2014 to 2015. He is currently an Associate Professor with the Department of Computer Technology, Anna University, Chennai, and also the Principal Investigator of the NGNLabs. He was a recipient of the Young Engineer Award from Institution of Engineers India in 2009 and the FastTrack Grant for Young Scientist from the Department of Science and Technology in 2011. He has given many invited talks across the globe and has chaired conference sessions. His current research interest includes 5G networks, LTE-advanced, IoT, network virtualization, SDN, wireless security, machine learning, mobile database, and data offloading. He is a Senior Member of the ACM and a Lifetime Member of CSI and ISTE.

ALI KASHIF BASHIR (M'15–SM'16) received the Ph.D. degree in computer science and engineering from Korea University, South Korea. He held appointments with Osaka University, Japan, the Nara National College of Technology, Japan, the National Fusion Research Institute, South Korea, Southern Power Company Ltd., South Korea, and the Seoul Metropolitan Government, South Korea. He is currently an Associate Professor with the Faculty of Science and Technology, University of the Faroe Islands, Faroe Islands, Denmark. His research interests include cloud computing, NFV/SDN, network virtualization, network security, IoT, computer networks, RFID, sensor networks, wireless networks, and distributed computing. He is an Editorial Board Member of journals, such as the IEEE Access, the *Journal of Sensor Networks*, and the *Data Communications*. He has Chaired several conference sessions, gave several invited and keynote talks, and reviewed the technology leading articles for journals, such as the IEEE Transactions on Industrial Informatics, the *IEEE Communication Magazine*, the IEEE Communication Letters, and the IEICE Journals and conferences, such as the IEEE Infocom, the IEEE ICC, the IEEE Globecom, and the IEEE Cloud of Things. He is serving as the Editor-in-Chief of the IEEE Internet Technology Policy Newsletter and the IEEE Future Directions Newsletter.

MASAYUKI MURATA (M'88) received the M.E. and D.E. degrees in information and computer science from Osaka University, Japan, in 1984 and 1988, respectively. In 1984, he joined the Tokyo Research Laboratory, IBM Japan, as a Researcher. From 1987 to 1989, he was an Assistant Professor with the Computation Center, Osaka University. In 1989, he moved to the Department of Information and Computer Sciences, Faculty of Engineering Science, Osaka University. In 1999, he became a Professor of the Cybermedia Center, Osaka University, where he is currently with the Graduate School of Information Science and Technology since 2004. He has over 400 papers of international and domestic journals and conferences. His research interests include network architecture, and performance modeling and evaluation. He is a member of the ACM and IEICE.